HASIL CEK_60020397_Point-C19-IRD-850GB-Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:52AM (UTC+0700)
Submission ID: 1471643554
File name: ecurity_in_university_based_on_framework_COBIT_5_using_CMMI.pdf (971.87K)
Word count: 4395
Character count: 23624

Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI Analysis of academic service cybersecurity in university based on framework COBIT 5 u...

Article *in* IOP Conference Series Materials Science and Engineering · May 2020

DOI: 10.1088/1757-899X/821/1/012003

CITATION
1

READS
82

3 authors, including:

Imam Riadi
Ahmad Dahlan University
193 PUBLICATIONS **891** CITATIONS
SEE PROFILE

Iwan Tri Riyadi Yanto
Ahmad Dahlan University
62 PUBLICATIONS **279** CITATIONS
SEE PROFILE

Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI

Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI

I Riadi[1,] *, I T R Yanto[1], and E Handoyo[3]

[1] Department of Information System, Faculty of Science and Applied Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[1] Department of Information System, Faculty of Science and Applied Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2] Department of Computer Engineering, Universitas Muhammadiyah Lamonggan, Indonesia

*Email: imam.riadi@is.uad.ac.id

Abstract. A secure academic information system is part of the college. The security of academic information systems is very important to maintain information optimally and safely. Along with the development of technology, academic information systems are often misused by some irresponsible parties that can cause threats. To prevent these things from happening, it is necessary to know the extent to which the security of the academic information system of universities is conducted by evaluating. So the research was conducted to determine the Maturity Level on the governance of the security of University Ahmad Dahlan academic information system by using the COBIT 5 framework on the DSS05 domain. The DSS05 domain on COBIT 5 is a good framework to be used in implementing and evaluating related to the security of academic information systems. Whereas to find out the achievement of evaluation of academic information system security level, CMMI method is needed. The combination of the COBIT 5 framework on the DSS05 domain using the CMMI method in academic information system security is able to provide a level of achievement in the form of a Maturity Level value. The results of the COBIT 5 framework analysis of the DSS05 domain use the CMMI method to get a Maturity level of 4,458 so that it determines the achievement of the evaluation of academic information systems at the tertiary level is Managed and Measurable. This level, universities are increasingly open to technological developments. Universities have applied the quantification concept in each process, and are always monitored and controlled for performance in the security of academic information systems.

1. Introduction

Companies or institutions place information technology as a thing that can support the achievement of the company's strategic plan to achieve the goals of the company or institution's vision, mission and goals. Information technology will get effective results if it uses good governance in its use and is able to be evaluated and evaluated [1]. Information systems are systems that contain SPD networks (systems processing data), which are equipped with communication channels used in data organization systems [2]. There are various concepts of information systems, compatibility is one of the keys to the successful implementation and acceptance of information systems [3]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats [4]. Academic

information systems must provide the security, privacy and integrity of data processed, so that the performance of academic information systems is also an important part that must be considered so that academic information systems can be used optimally and safely [5]. The application of information security systems aims to overcome all problems and constraints, both technically and non-technically which can affect the performance of the system such as availability, confidentiality and integrity factors so that the level of information security can be assessed [6] as in Figure 1.

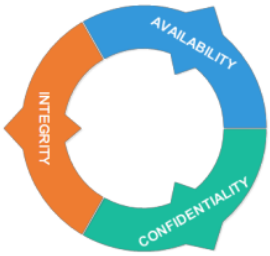

Figure 1 Information security aspects

The existence of a security problem triggers a procedure for controlling access rights to an information system [7]. A good information system security must apply the standard Deming cycle of quality [8]. The security of academic information systems can be audited with various standards such as COBIT, COSO, ITIL, CMM, BS779, ISO 9000. COBIT (Control Objectives for Information and related Technology) is a standard guide to information technology management practices and a set of best practices documentation for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues [8]. All organizations can adjust COBIT 5 for their various purposes, and are able to evaluate the organization in achieving its intended goals [9]. Domain DSS (Deliver, Service and Support) is related to system delivery and service support needed by the system, which includes service, security and continuity management, service support for users, and data management and operational facilities so that it is more integrated in the domain that provides services well [8].

DSS domains have sub-domain DSS05 wherein this sub-domain is a more intensive procedure for information security. The method that can be used in evaluating the achievement of evaluation is CMMI. Capability Maturity Model Integration (CMMI) is a model approach to assess the scale of capability and maturity of a software organization. The history of CMMI at the beginning was known as the Capability Maturity Model (CMM) which was built and developed by the Software Engineering Institute in Pittsburgh in 1987 [10]. The CMMI method in academic information system security is able to provide a level of achievement in the form of Maturity Level values. So as to be able to give a decision on the extent to which the security process of academic information systems that have been run by universities.

This study aims to conduct an evaluation related to the security management of academic information systems that have been implemented at Ahmad Dahlan University. This study aims to obtain the value of the level of information system security of an institution, so that recommendations and innovations can be made for the security of information systems in these institutions. So that the institution can provide security and comfort for the use of the information system.

2. Methods

2.1. DSS05 framework COBIT 5

The DSS05 sub-domain is part of the DSS domain (Deliver, Service and Support). As in Figure 2.

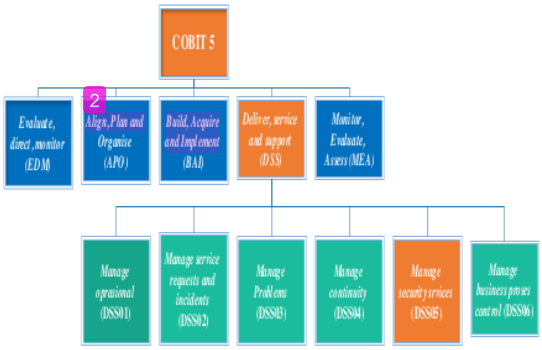

Figure 2. DSS05 scheme

The DSS05 sub-domain is managing security services where these sub-domains are grouped in 7 processes. The seven processes carry out some activities or statements of the 49 statements as follows [11]:

- Protect against malware (DSS05.01) where this process carries out and maintains existing precautions, detective and repairs (especially the latest security patches and virus controls) throughout the company to protect information systems and technology from malware (e.g., Viruses, worms, spyware, spam).
- Manage network and connectivity security (DSS05.02) where this process uses security measures and related management procedures to protect information from all methods of connectivity.
- Manage endpoint security (DSS05.03) where this process provides assurance of end points (e.g., Laptops, desktops, servers, and other cellular and cellular networks or software) guaranteed to be the same or greater than the requirements approved security.
- Manage user identity and logical access (DSS05.04) This process provides certainty for all users to have the right to access information in accordance with business needs. They and coordinate with the business division that manages access rights.
- Manage physical access to IT assets (DSS05.05) this process determines and applies procedures to give, limit and revoke access to physical buildings. Buildings and areas according to business needs, including emergencies. Access to buildings, buildings and areas must be justified, ratified, recorded and monitored.
- Manage sensitive documents and output devices (DSS05.06) where this process establishes physical security. In terms of documents relating to agencies. So that all output documents are standardized in security.
- Monitor the infrastructure for security-related events (DSS 05.07) where this process uses intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure that every event is integrated with monitoring events and managing events.

2.2 Capability Maturity Model Integration (CMMI)

CMMI has a streamlined assessment process. The assessment was based on questionnaires and was developed specifically to get software that could support process improvement. CMMI is a maturity method that can be used to improve processes within the institution. The purpose of using the CMMI within an institution is to improve the process of developing and improving the software product of the institution [12].

According to [13] CMMI has Capability Level. Capability Level is a model to describe how each core process runs within an institution. Capability Level has 6 levels for each core process, namely. As in Figure 3.

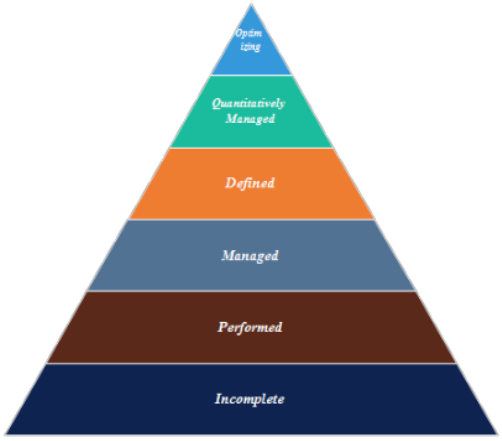

Figure 3. Capability level CMMI

According to [13] The CMMI model places, institutions in 5 Maturity Levels or CMMI levels, namely. As in Figure 4.

Figure 4. Maturity level CMMI

3. Result and discussion

This section will present a structured process method. Analysis of the implementation and measurement of the maturity level of the information system with the framework COBIT 5 sub-domain DSS05 and CMMI.

3.1 Observation of the academic information system process

This process conducts interviews directly with the resource person who has authority in the security of the academic information system at University Ahmad Dahlan, where the results are that BISKOM UAD uses an academic information system to be active in 2008, the beginning of the information system created and developed by vendors (Gama Techno) after that, in 2017 it was able to migrate to a new system where the system was developed by BISKOM UAD itself. Where in this migration is due

to the development of information systems technology, so it is considered necessary to do the migration to maintain the stability and security of the information system.

The purposes of the academic system of University Ahmad Dahlan are:

- To manage academic activities in University Ahmad Dahlan.
- Providing convenience to the community, namely lecturers, students, staff and BAA in the academic process.

As time goes on the use of information systems also experiences, obstacles, problems and threats to information systems. The problems, obstacles and threats that often occur are as follows:

- There are several systems that have not been well integrated.
- When the online KRS happened the server was down.
- It often happens to forget your username and password.
- The process of data connection or transmission is slow.
- Virus and malware attacks.

The BISKOM UAD standardization and audit process applies ISO 9000 where the standard is used for standards for quality management systems (SMM) which are aggregated with all bureaus in all institutions. This process also discusses the determination of respondents who will provide detailed information related to information on the security of existing academic information systems. The selection of respondent samples using purposive sampling technique, which is the selection of respondents 'samples determined by researchers on the grounds that identification of respondents' samples is done by referring to personal competencies that interact directly with IT governance [14]. Interviews get 2 respondents who are directly concerned with the field of information system security within the institution.

3.2 DSS05 mapping based on the COBIT framework 5

This process is a compilation of DSS05 domain conformity activities with questions to be made in the questionnaire. because of the limitations of our writing, we only list one of the 7 DSS05 sub-domain processes, namely DSS05.01. The DSS05.01 process consists of 6 activities, as in Table 1**.**

Table 1. Protect against malware activity

Protect against malware (DSS05.01)	
No.	**Activity Questions**
1	Obtain information about malicious software and how to handle it..
2	Install and activate anti-virus on your PC.
3	Is anti virus on the PC always updated.
4	Regularly review and evaluate information about potential malware threats
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information
6	Conduct periodic training on malware in the use of e-mail and the Internet.

Preparation of Questionnaires with a combination of DSS05 and Capability Level. This process is carried out by questionnaires based on the standard on DSS05 Framework COBIT 5 by combining with the capability level of CMMI standards so that the form of a questionnaire can be obtained that is able to answer the needs of the information system security in the installation. To simplify the reading process, the color differences for each decision are made in Capability Level and Maturity Level as in Table 2.

Table 2. Process color maps

Color	Information	
	Capability Level	***Maturity Level***
Red	*Incomplete*	*Non-Existent Initial*
Purple	*Performed*	*Initial / Ad Hoc*
Yellow	*Managed*	*Repeatable But Invinitve*
Blue	*Defined*	*Define Process*
Orange	*Quantitatively Managed*	*Managed and Measurable*
Green	*Optimizing*	*Optimized*

Where in this questionnaire there are 6 assessments for processes with capability level CMMI as in Table 3.

Table 3. Assessment of IT processes with CMMI capability level

Value	***Capability Level CMMI***	**Proses TI**
0	*Incomplete*	Are not done
1	*Performed*	Done, not periodically
2	*Managed*	Performed periodically
3	*Defined*	Done with SOP
4	*Quantitatively Managed*	Performed and monitored
5	*Optimizing*	Done, monitored and developed

The assessment of the IT process in Table 3 is combined with the standard COBIT 5 DSS05 framework in Table 1, as in Table 4.

Table 4. Questionnaire form

Protect against malware (DSS05.01)							
Activity		**Answer**					
		0	**1**	**2**	**3**	**4**	**5**
1	Obtain information about malicious software and how to handle it.						
2	Install and activate anti-virus on your PC.						
3	Is anti-virus on PC always updated.						
4	Regularly review and evaluate information about potential malware threats.						
5	Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information.						
6	Conduct periodic training on malware in the use of e-mail and the Internet.						

3.3 Calculation of security SIA maturity level

This section will explain the results of the analysis of the implementation and measurement of the performance of the maturity level of academic information systems obtained from the results of questionnaires and interviews in accordance with the framework 5 COBIT domain DSS05. To identify the extent to which the company or organization meets good information security standards, can use

the framework identification represented at a level of maturity that has a level of grouping capability of the company, as described in Table 5.

Table 5. Value of maturity level criteria

Criteria	Information
0 – 0.50	*Non-Existent Initial*
0.51 – 1.50	*Initial / Ad Hoc*
1.51 – 2.50	*Repeatable But Invinitve*
2.51 – 3.50	*Define Process*
3.51 – 4.50	*Managed and Measurable*
4.51 – 5.00	*Optimized*

The results of the questionnaire that has been given to the respondent and filled in by the respondent get results. Because the page is limited, the data displayed is only on DSS05.01. As in Table 6.

Table 6. The results of the questionnaire

DSS05	Respondent 1	Respondent 2
DSS05.01.1	5	5
DSS05.01.2	5	5
DSS05.01.3	5	5
DSS05.01.4	5	5
DSS05.01.5	5	5
DSS05.01.6	5	5

Furthermore, the correlation between level values and absolute values that are done by calculation in the form of an index uses a mathematical formula. The mathematical equation to determine the index value is as follows [15]:

$$Indeks = \frac{\sum Most\ Question\ Answers}{\sum Questionnaire\ Questions} \quad (1)$$

After getting the index, we can get the current Maturity Level (present). This value is the accumulated value of the process that is running on the institution as in Table 7.

Table 7. Existing maturity value

DSS05	*Value of Maturity Level Existing*
Protect against malware	5.00
Manage network and connectivity security	5.00
Manage endpoint security	4.39
Manage user identity and logical access	4.88
Manage physical access to IT assets	4.64
Manage sensitive documents and output devices	3.10
Monitor the infrastructure for security-related events	4.20

3.4 Gap maturity level calculation

Once the existing Maturity Level values are obtained and Maturity The recommendation level (target) has been determined, then the gap between the current condition and the target to be achieved will be analyzed and identified opportunities from the gap to be optimized. Level gap as in Figure 5**.**

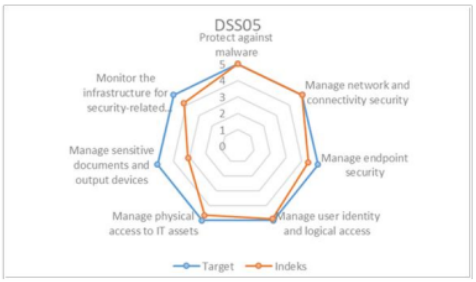

Figure 5. Maturity level gap

3.5 Gap analysis maturity level

Based on Gap analysis obtained from the results of the target level to be achieved and the level achieved on DSS05, as in Figure 5**.**, then here is some Gap Maturity Level Analysis. As in Table 8 as follows.

Table 8. Gap maturity level analysis

DSS05	***Maturity Level***
Protect against malware	*Optimized*
Manage network and connectivity security	*Optimized*
Manage endpoint security	*Managed and Measurable*
Manage user identity and logical access	*Optimized*
Manage physical access to IT assets	*Optimized*
Manage sensitive documents and output devices	*Define*
Monitor the infrastructure for security-related events	*Managed and Measurable*

The overall value of Maturity Level on DSS05 will be calculated on average so that it will get the level of Maturity Level in the organization or institution.

$$Maturity\ Level\ DSS05 = \frac{\sum Maturity\ Level}{many\ processes} \quad (2)$$

$$MLDSS5 = \frac{\begin{array}{c} i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + \\ i(DSS05.04) + i(DSS05.05) + \\ i(DSS05.06) + i(DSS05.07) \end{array}}{mp}$$

$$MLDSS05 = \frac{5 + 5 + 4{,}388 + 4{,}875 + 4{,}642 + 3{,}1 + 4{,}2}{7}$$

$$Maturity\ Level\ DSS05 = 4{,}458$$

From the calculation results obtained the value of achievement is 4,458 so that it can be set Maturity Level of organization or institution is at the Managed and Measurable level.

3.6 Compilation of IT governance recommendations

After Maturity Level has been determined, the recommendation preparation process will be carried out. Recommendations that can be given to improve the quality of information system security in the agency:

- Protect against malware (DSS05.01) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to perform procedures well and is able to develop malware related ones. It is expected that the agency will be able to anticipate the threat of malware more quickly and precisely in detecting malware threats.
- Manage network and connectivity security (DSS05.02) is at the level of Optimized wherein at this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures well and is able to carry out developments related to security of activities. Establish a system that is used to evaluate threats that will arise, documented and monitored. It is expected that the future agencies will be better prepared with the threat of connectivity and be able to quickly provide countermeasures related to connectivity security.
- Manage endpoint security (DSS05.03) in the Managed and Measurable level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures well, only agencies must carry out routine evaluations, at least once a month on information systems that are feared to be potential new threats.
- Manage user identity and logical access (DSS05.04) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures properly and is able to develop related access rights of each user. It is expected that companies or institutions are able to provide early warning of the potential security threats to the system and equipment that is owned by all employees.
- Manage physical access to IT assets (DSS05.05) is on the Optimized level where in this level the BISKOM of Ahmad Dahlan University has been able to perform procedures well and is able to carry out development related to physical security. It is hoped that in the future, it will be able to produce and report related to security system trials that are applied and evaluated in a periodic physical shutter.
- Manage sensitive documents and output devices (DSS05.06) in the Define Process level, in this BISKOM, Ahmad Dahlan University has implemented physical security, accounting practices in terms of documents relating to the situation. So that all output documents are standardized in security. It's just hoped that later it will be able to bend documentation and evaluate existing threats.
- Monitor the infrastructure for security-related events (DSS05.07) is in the Managed and Measurable level where in this level the BISKOM of Ahmad Dahlan University has been able to carry out procedures properly using intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure that every event is integrated with monitoring events and management of events must carry out routine evaluations, at least every semester to the information system which is feared that potential new threats can arise.

4. Conclusion

Sub-domain DSS05 Manage security services is a good procedure to be used in the implementation and mega-audit related to the security of academic information systems and CMMI is a good assessment method in an institution's audit system. Based on the research conducted at the BISKOM, Ahmad Dahlan University received a Maturity Level of 4,458 thus stipulating that the current maturity level is on the Managed and Measurable level. This level, institutions are increasingly made aware of technological developments. Institutions have implemented the quantification concept in each process, and are always monitored and controlled for performance.

References

[1] Riadi I and Handoyo E 2019 Security analysis of GRR Rapid Response Network using COBIT 5 Framework vol **10** no 1 pp 29–39.
[2] Fathoni L F, Muslihudin, Kartika F and Anton Y 2016 Application information system based health services android *J. Ilmu Tek. Elektro Komput. dan Inform* vol 2 no 1 pp 39–48.
[3] Muslimin I, Hadi S P and Nugroho E 2017 An evaluation model using perceived user technology organization fit variable for evaluating the success of information systems vol **4** no 2 pp 86–94.
[4] Riadi Y W I and Yudhana A 2016 Webserver security analysis using the penetration testing method *in Annual Research Seminar 2016* vol **2** no 1 pp 300–4.
[5] Kurniawan E and Riadi I 2003 Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-CMM *Int J Comput Sci Inf Secur*. vol **16** no 1 pp 139–47.
[6] Rosmiati I. R and Prayudi Y 2016 A maturity level framework for measurement of information security performance *Int J Comput Appl* vol **141** no 8 pp 975–8887.
[7] Hermaduanti N and Riadi I 2016 Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN *J Theor Appl Inf Technol* vol **93** no 2 pp 287–96.
[8] Hicham E, Boulafdour B, Makoudi M and Regragui B 2012 Information security *4th wave," J. Theor. Appl. Inf. Technol* vol **43** no 1 pp 1–7.
[9] Latifi F and Zarrabi H 2017 A COBIT5 framework for IoT risk management *Int J Comput Appl* vol **170** no. 8 pp 40–3.
[10] Konttinen V 2016 Towards Disciplined Software Development no May.
[11] Andry J F 2016 Audit of IT governance based on COBIT 5 assessments: A case study *J. Teknol. dan Sist. Inf* vol 2 no 2 p. 27.
[12] P. D. Syafitri, "Assessment of Quality of Information System Development at Distributor Companies," J. Sist. Inf. Bisnis, vol. 10, no. 01, pp. 15–27, 2016.
[13] CMMI Product Team, CMMI® for Development, Version 1.3. 2010.
[14] P. Rahayu and D. I. Sensuse, "Assessment of e-Government Implementation in the Ministry of Education and Culture's PUSTEKOM based on the PEGI method," J. Sist. Inf. Bisnis, vol. 02, pp. 139–145, 2017.
[15] Prasetyo A and Mariana N 2011 Analysis of information governance (It Governance) in the academic field with Cobit FrameWork Case study at Stikubank University Semarang *J. Teknol. Inf. Din* vol **16** no 2 pp. 139–49.

HASIL CEK_60020397_Point-C19-IRD-850GB-Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI

ORIGINALITY REPORT

10%	9%	6%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	khan-muhammad.github.io Internet Source	1%
2	Yassine Maleh, Abdelkebir Sahid, Mustapha Belaissaoui. "chapter 3 Evaluation of IT Governance in Middle East and North African Large Organizations", IGI Global, 2019 Publication	1%
3	Submitted to University of Melbourne Student Paper	1%
4	Submitted to HELP UNIVERSITY Student Paper	1%
5	www.govpage.co.za Internet Source	1%
6	Submitted to Colorado Technical University Online Student Paper	1%
7	I Gede Ary Suta Sanjaya, Gusti Made Arya	

	Sasmita, Dewa Made Sri Arsa. "Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City)", International Journal of Computer Network and Information Security, 2020 Publication	1%
8	ejournal.nusamandiri.ac.id Internet Source	1%
9	idoc.pub Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		